

REMARKS

Claims 86-91 are now pending in the above-captioned application.

RESPONSE TO PREVIOUS AMENDMENT

The Examiner has withdrawn the rejection of claims 1 and 32 under 35 U.S.C. §112, in view of Applicant's previous Amendment. However, the Prior Art rejections were repeated *verbatim* and were made FINAL. Applicant herewith files a Request for Continued Examination (RCE) to reopen prosecution on the merits to further consider this Prior Art rejection in view of applicant's arguments and amendments to the claims.

RESPONSE TO EXAMINER'S ARGUMENTS

The Examiner has repeated all of the art rejections *verbatim* in the Office Action of November 4, 2008 and made the action FINAL. The Examiner has responded to applicant's previous arguments, and that response is conveniently presented in the first section of the Office Action.

Applicant's previous arguments concerning the Prior Art references are incorporated herein.

As all of the claims have been cancelled and new claims presented, many of the previous arguments are now *moot*. New claims 86-91 have been added, which combine features of a number of the previous claims and refine the claim language (e.g., eliminate "means" language), in order to more clearly distinguish the present invention over the Prior Art of record.

However, as the new claims are based on elements of the previous claims, some of the arguments presented in the previous Office Action are still relevant and will be addressed herewith.

Applicant would like to thank the Examiner for grouping the response to these arguments conveniently at the beginning of the Office Action so they can be more readily addressed. Some of the Examiner's arguments and concerns have merit and bear comment.

I. "Remote" Computer issue:

This argument is boiling down to a dispute over the meaning of the term "remote", which does not appear to be an argument that will be readily resolved. When a §103 rejection boils down to arguing dictionary definitions of claim terms, it may be more suitable to amend the claims instead. Even in the computer arts, historically, something as simple as a disc drive or a printer could be considered a "remote device". So the term "remote" by itself may be insufficient to distinguish the present invention from the Prior Art.

In addition, although the cited portion of Volnak did not disclose components being "remote" as in the present invention, other Figures of Volnak, such as Figures 9B and 9C appear to show "remote" components. However, in the present invention, it is not mere physical remoteness (regardless of the definition of that term) that insures inviolability of the diary alone, but also the *independent* operation of the archive.

The present invention provides a secure Diary, and one point of the claimed invention is that the user cannot alter the diary at whim. If the user could alter the Diary at whim, he would be able to delete entries and alter entries, and as such, the Diary would have no use for many applications, such as in legal proceedings, as the contents could not be considered trustworthy. Thus, the present invention provides the Diary Archive at a remote and independent location. If the Archive was in the user's computer, the user could destroy the Archive at will. Even if the Archive were encrypted, encoded, or otherwise "locked" to prevent a user from altering it, the user could still destroy the Archive simply by destroying or discarding the computer or hard drive or other component.

However, with the Archive being remotely located, and independently operated, the data is unalterable and thus forms a permanent or semi-permanent record. Such a Diary Archive has uses for legal documents, government records, financial records, and the like, where the inviolability of the record is important. A paper document leaves evidence of alteration. An electronic document, however, can be more readily compromised. In the present invention, by making the Diary Archive remote from the user, security is physically provided.

Claim 86 includes the limitation that the Diary Archive is "remote and independent" from the user. In addition, this Diary Archive is recited as *"preventing anyone, including the user, from modifying and from deleting said one or more data blocks stored at said remote diary archive"*. Thus, it is clear that

applicant is not merely arguing that mere "remoteness" is the point of novelty here, but the combination of the Archive being physically remote and also independent from the user - or anyone else.

As will be discussed in more detail below, none of references of record teach or suggest this remote and independent archive that prevents even the user from modifying and from deleting an entry.

Note that applicant has changed the language to "modifying **and** from deleting". In the original claims, the term "modifying ~~or~~ deleting" was used, which arguably would be a Markush group, which, presented as a negative limitation ("preventing a user from...") could be satisfied by a reference teaching either feature (e.g., a reference showing the prevention of modification ~~or~~ deletion). However, in the present invention, deletion is merely a special case of modification. In order to make the diary inviolable, it is required that the user not be allowed to modify **and** not be allowed to delete an entry. The revised claim language reflects this change.

2. Interpretation of Sykes

The Office Action argues that the portions of Sykes cited by applicant were not cited in the Office Action, and thus not relevant. Applicant respectfully disagrees. One cannot take the teachings of a reference out of their context to argue that they teach the invention. Thus, one cannot dismiss portions of Sykes that are not helpful to his rejection merely on the grounds they were "not cited" in the Office Action.

The Office Action further argues that applicant's comments concerning Sykes "delete" function are "spurious" as a "delete" function is not claimed in claims 1 and 32 (Office Action of 11/04/08, Page 2, lines 12-15). In this regard, the Examiner is at least partially correct. Claims 1 and 32 did not recite a "delete" function, rather they recite a **"non-delete" function**, so to speak. New claim 86 contains a similar limitation:

"remote diary archive storage, coupled to the network and located physically remote from and independent from the user, for receiving and storing the one or more data blocks, **said remote diary archive storage preventing anyone, including the user, from modifying and from deleting said one or more data blocks** stored at said remote diary archive to provide non-rescindable storage of user diary entries, where the user negotiates **an initial**

time period with the remote diary archive to reach agreement on the initial time period for **non-rescindable storage** of said one or more data blocks;"

In other words, the archive of the present invention *prevents* users from deleting or modifying elements in the archive, at least within an initial time period for non-rescindable storage. **Sykes teaches that a user can delete data at any time.** Thus, Sykes clearly does not teach or suggest a non-rescindable (non-deleteable) archive. The Rejection cannot simply ignore portions of the reference, which clearly show that Sykes does not teach the invention.

3. Official Notice Rejection

With regard to claim 70, the Examiner argues that since applicant did not explicitly state why his Official Notice elements were **not** common knowledge, the traversal fails, and the elements argued as "Official Notice" are now admitted Prior Art. Applicant disagrees with this contention. However, the point is moot as claim 70 has been cancelled and the limitation does not appear in new claims 86-91.

4. Time-Stamping Means

The Examiner points out that that Page 6 of the Office Action did set forth the portions of the reference which he claims set forth the time-stamping means. Applicant apologizes for this oversight and has reviewed the reference in view of the Examiners comment and requests the Examiner reconsider the rejection in view of the present amendment and the comments below.

5. Predictable Results

The Examiner argues that the time-stamping means is not recited as interacting with the other elements of the claim, and thus produces a predictable result. This point is well taken, and Applicant has presented new claims herein to more closely tie these elements together. Applicant respectfully requests reconsideration of the rejection in view of the present amendment and the comments below.

6. Filing Key

The Examiner argues that the term "filing key" can comprise a keyword, as defined in Applicant's Specification. Paragraph [0074] of the present Specification does indicate that the filing key may comprise a keyword. However, applicant submits that the term as used in the Prior Art is used in a different manner than in the present invention. But moreover, the point, with regard to the independent claim, is moot, as this limitation is not a feature of the new independent claim, which is distinguishable over the art of record without the filing key limitation.

REVIEW OF PRIOR ART REJECTIONS

As the previous claims have been cancelled, the Prior Art rejections are now moot. New claim 86 is based on previous claims 1, 4, 5 and 6, in that it includes the limitations of a remote diary archive with a negotiable period of non-rescindability, an encryption site, a digital signature generator, and a time-stamping generator. The Examiner had previously applied the combination of Volnak, Sykes, Botti and Cane against these claims in combination. Thus, applicant will address the rejection of the *combination* of Volnak, Sykes, Botti, and Cane with regard to the new claims, and in particular, independent claim 86.

The combination of elements in new claim 86 provides a secure archive for a secure diary, which cannot be altered by anyone, even the author. Encryption, remote and independent from the archive, prevents the archive from reading the diary entry. The digital signature establishes that the user submitted the entry. The archive, by its non-rescindable nature, prevents alteration or deletion of an entry by the user. The use of the time-stamp helps prevent any alteration from being undetected. Being remote and independent from the user and archive, the signature and time-stamp generators cannot be tampered with by the user and archive. Hence it is more difficult for the user to falsify a time stamp, or for the archive to falsify a digital signature or a time-stamp.

Also, should a user device containing encryption, digital signature, and time-stamping software and hardware be lost or stolen, the guilty party might use the device to forge a document, store it on the archive, and falsely attribute it to the user. Such actions could be more difficult to accomplish when these services are remote and independent.

As a result, the present invention provides a secure diary, which provides an inviolable time-stamped record, digitally signed by the user, that cannot be deleted or altered, even by the user, for a negotiated initial time period, and which cannot be read by anyone except the user. This combination of elements produces an unexpected result, when compared to the references cited in the rejections, as the combination of elements provides a level of security that the individual references, when combined, do not provide. In part, this is due to the addition of another element - the independence of each component, which is not taught by any of the references.

The remote digital signature, time stamping, and encryption are also useful because they enable diary entries to be made from anywhere, cell-phone or Internet cafe, for example. Thus, the present invention can be made portable, such that the user device does not need to include a time-stamping mechanism, encryption, or archive.

Applicant will address each element of claim 86 and the corresponding reference(s) previously applied to the claim element.

Non-Rescindability

While Volnak discusses "freezing" his entries, it is not clear how these "frozen" entrees can be preserved. Moreover, the entire entry is not "frozen" but rather a portion of it may be edited:

"Tag text field 570 is the only field that can still be modified after the entry is frozen (e.g., in a notebook entry)." (Volnak, Col. 7, lines 14-16, emphasis added)

Volnak, however, does not discuss that the archives of the group library are **independent** and contracted to perform for the user.

Volnak is trying to develop a better method of working with data: "Typically, however, database management systems do not allow users to manipulate the results of the queries, although some database management systems allow users to sort the order in which the records returned by a query are displayed. Other systems allow users to combine multiple search parameters in a single query; however, this approach still requires a new search to be performed. Accordingly, there is a need for a computer information system that allows results of searches to be manipulated and stored for future use, without requiring a new search to be performed." (Column 1, lines 34-44.)

Volnak is working in the context of databases. Typically in such systems, a security bit is set for a data element to indicate whether or not the element can be modified (See, e.g. "unix security" on Wikipedia). Different bits are set to indicate by whom an element can be modified. Usually there is a user, typically the chief system programmer, who has privileges to change any such bit and hence can modify any data element. Such a chief system programmer, of course, will do as his superior, the owner, suggests. This is almost certainly the context in which Volnak is working since Volnak makes no references to encrypted time stamps and digital signatures which are required for higher levels of security than provided by requiring high privileges to change security bits.

In diary systems in the art, the owner or anyone is prevented, by e.g. physical seals or firmware from being able to make these alterations. In the present invention, *it is the negotiated agreement with a remote, independent archive, which prevents the owner of the data from being able to change the data.*

As noted above, an indication of the fact that Volnak is working in a database context is that nowhere does he refer to digital time stamping or to digital signatures. These are the means in the art by which any user, including an archives systems programmer, is prevented from undetectably modifying an entry. Volnak also makes no reference to encryption, which could prevent someone other than the user from reading an entry. As such, it would not be "obvious" to apply digital time-stamping, digital signature, or encryption to Volnak, as Volnak does not need, teach or suggest such features - as his system does not require nor could make use of them (and in fact, such features may inhibit operation of his system). As these features produce a new and unexpected result in the present invention (provide a secure archive) they are not merely tacked-on elements producing no unexpected result.

Botti explicitly teaches that the archived data may be altered by the user (See, Botti, Abstract). Botti teaches only that a CRC or checksum can be used to detect an alteration.

As noted above, Sykes explicitly states that records can be deleted at will in his system. As noted in applicant's previous responses, Cane provides ((Summary of Invention)) for deletion of entries at any time.

Thus, none of the four references cited teach or suggest a non-rescindable entry on a remote archive.

Time Period for Non-Rescindability

The previous Office Actions admit that "Volnak does not explicitly teach wherein the user negotiates the initial time period with the remote archive storage means to reach agreement on an initial time period for non-rescindable storage of said one or more data blocks".

The Office Actions argued "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the non-rescindable remote archive system of Volnak with the ability to negotiate a time period of archive storage as described by Sykes." Again, applicant's previous comments regarding Sykes are incorporated herein.

Sykes recites:

"The email message remains stored with the third party archiving and verification provider **for a time determined by the sender's user profile**, which was established at the time the sender opened its account, as from time to time amended. Alternatively, the user could be allowed to select the time for storage at the time the message is sent. The user can also extend the time for storage later, as described below. The third party verification provider preferably provides the sender with access to the stored email messages via a web browser, **allowing the sender to manage the stored messages, deleting unneeded messages**, extending the storage time for messages, and requesting verified copies of messages." (Sykes, Col. 6 lines 7-19, emphasis added)

Claim 86 recites, in part:

". . . said remote diary archive storage **preventing anyone, including the user, from modifying and from deleting said one or more data blocks** stored at said remote diary archive for at least an initial time period,"

As Sykes allows the user to **delete** messages, even during the archiving time period. In contrast, the present invention prevents the user from deleting and modifying data blocks during the initial time period. This deletion-prevention function is useful for a diary, as if the user were allowed to delete entries at will, the integrity of the diary is compromised.

Thus, it is clear that Sykes does not fix the problem with the underlying Volnak reference. In particular, Sykes does not teach or suggest a non-rescindable archive, but in fact, teaches that entries may be deleted at will. There is no description in Sykes of negotiating an initial time period for non-rescindable storage of data blocks, as set forth in claim 86.

Encryption Site

New claim 86 recites a remote and independent encryption site, which encrypts the data blocks from the user's diary and then stores in them in the remote diary archive. The purpose of the encryption is to keep the owner of the archive from reading the entry. This is also the reason that the encryption party, must be remote and independent of the archive. Of course the encryption party must be remote from the user, and connected by communication means, otherwise the user would have to be in possession of an encryption device whenever he/she wanted to archive a diary entry in order to make it impossible for the archive to read it.

The Office Actions admit that Volnak and Sykes do not teach an encryption site, and an encryption site whereby the remote storage archive may not decrypt the blocks. Cane is added to the mix to allegedly show this feature. Cane is directed toward an archiving system (e.g., backup up your hard drive on the internet) and thus allows a user to archive their data to the Cane archive server in encrypted form, where the archive server cannot decrypt the data. Cane is alleged to teach a cryptographic engine 14 in Figure 1 coupled to a user (Figure 1, source system 8) at one end of a communication link, and, via the same communication link, to a remote archive storage (Archive Server 30).

Hence the encryption of Cane is not performed by a party remote and independent of the user and the archive, but by a system coupled to the user at the same end of the communication link.

Combining Cane with Volnak and Sykes does not produce the results of the present invention with respect to encryption.

Digital Signature Generator

Botti was applied in the rejection of the previous claims to show a digital signature generator. However, the Office Actions admit that none of Volnak, Sykes, or Botti teach a **remote and independent** digital-signature generator, but argues that it would be obvious to add such a feature, absent some unexpected result. Again, Applicant disagrees with this interpretation of the motivation to combine aspect of §103. The burden is on the Examiner to show a motivation to combine the elements, not on the Applicant to show why the elements cannot be combined.

However, in the present invention, the use of an independent, remote digital signature generator insures the integrity of the diary. Any locally used device, regardless of the cleverness of encryption, can be compromised by someone who steals a user device by the fact of physical access to the device. With this access a fraudulent diary entry could be created and stored on the archive. By removing this aspect of the diary from the user's computer, and providing it from an independent third party, the overall security of the archived diary is enhanced.

And a remote digital signature site can be used over a communication system without access to any particular user device.

In addition, since the digital signature generator is remote from the archive, if the archive wanted to create a fraudulent entry, they would have to hack a remote, independent digital signature site, not to mention independent time-stamp and encryption sites.

Time Stamp Generator

Claim 86 further includes the limitation of a time-stamp generator, which is remote from both the diary input and archive, for providing a time-stamp, which is added as a non-rescindable data block. The Office Action argues that Volnak teaches such a time-stamping means in Col. 7, lines 3-15, which recite a "creation time label 580". Volnak describes this element *in toto* as follows:

"Source text label 575 is a non-modifiable text label identifying the source of the entry. Likewise, **creation time label 580 is a text label indicating the creation time of the entry.**" (Volnak, Col. 7, lines 16-19, emphasis added)

While arguably, this "creation time label" could be considered a "time stamp", Volnak does not teach or suggest having such a time-stamp generated by a third party, nor does he teach or suggest an encrypted, secure time-stamp. A simple time-stamp generated on a user computer can be counterfeited later easily if the user merely resets the clock on their computer. Thus, diary entries can be deleted by the owner's system programmer in the typical computer systems that, in the absence of references we must assume that Volnak contemplates. The diary entries and time stamps may be deleted by the user himself in Sykes (as described above), and then retroactive diary entries and back-dated time stamps created, and thus a false record manufactured.

In addition, a secure digital time stamp is needed in a diary, even if the archive is perfect, because it enables one to verify that a diary entry was made by the author on a particular date even if the diary entry is removed from the archive. This is not a requirement for Volnak, and he does not cite references for a secure digital time stamp, but is a very desirable feature for a digital diary. After all, it would not be convenient for the user, much less a third party, to validate the timestamp and to examine the decrypted diary directly on the archive, where, very likely there would be access restrictions and where the data are likely encrypted. A third party can receive from the user/author the decrypted diary entry, digital time stamp and digital signature and can verify those data on their own computer, and thus authenticate the entry.

In response to Applicant's previous arguments, the Examiner points out that absent some unexpected result, the addition of a time-stamp is obvious in view of the Prior Art. While Applicant does not agree that this argument accurately reflects the standard of obviousness under the law (the burden is on the *Examiner* to provide the motivation to combine, not on the *Applicant* to show a non-motivation or unexpected result), applicant does note that the time-stamp of the present invention does in fact operate in a manner different than expected from Volnak, Sykes, or Botti, alone or in combination.

In the present invention, diary entries cannot be modified or deleted for a predetermined time period. As they are located on a remote and independently operated archive, the user cannot modify or destroy them. As the time stamps are generated by an independent party, they cannot be compromised or spoofed either. As such, once a user creates a diary entry, its integrity is insured by the location in a remote and independent archive. The time-stamp, being generated *and encrypted* by a remote and independent third party, cannot be compromised either.

As noted above, a "local" diary (Volnak, Sykes, Botti) can be readily compromised by merely deleting an entry (which Sykes explicitly provides for, and Volnak and Botti do not insure against) from a file and substituting a new entry using a faked time-stamp, which can be easily done merely by resetting the clock on a local computer and then generating the entry.

Volnak's time stamp is not a secure time stamp, as discussed above and as is required for a diary. If it were remote and independent that could help it to be secure, but that would not be sufficient; the accurate time would still have to be added to the entry or to the hashed entry and then digitally signed. None of this is suggested or referenced by Volnak. And he does not have to do so, since there is no plausible need for a secure time stamp for his application.

Thus, the use of the remote and independent third party encrypted time-stamp does indeed produce a result different from (and an improvement from) Volnak, Sykes, Botti, and Cane, taken alone or in combination.

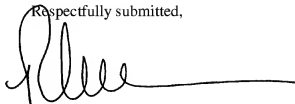
CONCLUSION

New claim 86 recites a combination of elements, which provides a secure archive for a diary, which cannot be altered by anyone, even the author, as in order to alter any entry, participation by a number of parties (e.g., archive, encryption site, digital signal generator, time-stamping generator) would be required. As a result, the present invention provides a secure diary, which provides an inviolable record that cannot be deleted or altered, even by the user, for a negotiated initial time period. This combination of elements produces an unexpected result, when compared to the references cited in the rejections, as the combination of elements provides a level of security that the individual references, when combined, do not provide. In part, this is due to the addition of another element - the independence of each of the components, which is not taught by any of the references.

As none of the references, taken alone or together, teach all of these elements of claim 86, and since the combination of elements in claim 86 produces a result not expected, applicant submits that all of claims 86-91 are allowable over the Prior Art of record. An early Notice of Allowance is respectfully requested.

The Commissioner is hereby authorized to charge any additional fees associated with this communication, including patent application filing fees and processing fees under 37 C.F.R. § 1.16 and 1.17, or credit any overpayment to **Deposit Account No. 50-1393**.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'R. Bell', followed by a long horizontal line extending to the right.

Robert Platt Bell
Registered Patent Attorney
P.O. Box 13165
Jekyll Island, Georgia 31527

Robert P. Bell
Registration Number 34,546

(703) 474-0757